AMENDMENTS TO THE CLAIMS

1. **(Currently Amended)** A semiconductor memory card comprising a tamper resistant module that is tamper resistant and ~~a nontamper resistant memory that is~~ a nonvolatile memory that is not tamper resistant,

wherein the tamper resistant module includes:

an internal memory having a usage area used by a program stored in the tamper resistant module; and

a processing unit including a virtual machine and an operation system, the program being an application executed by the virtual machine,

wherein when requested by the program, the processing unit is operable to (i) assign an area in the ~~nontamper resistant~~ nonvolatile memory that is not tamper resistant to the program, and (ii) generate, [[on]] in the internal memory of the tamper resistant module, access information for the assigned area in the ~~nontamper resistant~~ nonvolatile memory that is not tamper resistant, ~~and~~

wherein the assigned area in the ~~nontamper resistant~~ nonvolatile memory that is not tamper resistant is for a portion of confidential data to be written in, the portion of confidential data being used by the program and read by referring to the access information existing in the internal memory of the tamper resistant module,

wherein the internal memory stores a first area table indicating a location and a size of the usage area,

wherein the nonvolatile memory that is not tamper resistant stores a second area table indicating a location and a size of the assigned area in the nonvolatile memory that is not tamper resistant, the second area table being encrypted using a predetermined encryption key, and

wherein the access information is a set of the predetermined encryption key and information indicating a location of the second area table.

2. **(Canceled)**

3. **(Currently Amended)** A semiconductor memory card according to Claim 1, wherein

the processing unit comprises:

an assigning unit operable to assign, at a time of the generation of the access information, an encryption key which the program uses in accessing the assigned area in the ~~nontamper-resistant~~ nonvolatile memory that is not tamper resistant;

an encrypting unit operable, at a time of the program writing data to the assigned area in the ~~nontamper-resistant~~ nonvolatile memory that is not tamper resistant, to encrypt the data; and

a decrypting unit operable, at a time of the program reading data from the assigned area in the ~~nontamper-resistant~~ nonvolatile memory that is not tamper resistant, to decrypt the data.

4. **(Original)** A semiconductor memory card according to Claim 3, wherein

the processing unit further comprises:

a receiving unit operable to receive a security level from the program; and

a storage unit that stores values for different security levels, bit lengths of an encryption key, and encryption methods, the bit lengths and encryption methods corresponding one-to-one to the values,

the encryption key assigned by the assigning unit is generated based on a bit length corresponding to the received security level, and

the encryption and decryption by the encrypting unit and decrypting unit, respectively, are performed based on an encryption method corresponding to the received security level.

5. **(Canceled)**

6. **(Currently Amended)** A semiconductor memory card according to Claim [[5]] 1, wherein

the ~~nontamper resistant~~ nonvolatile memory that is not tamper resistant includes a first memory module and a second memory module, and

a unit of writing in the second memory module is smaller than a unit of writing in the first memory module, and the second memory module stores file management data.

7. **(Original)** A semiconductor memory card according to Claim 6, wherein

the second memory module is one of a Ferroelectric Random Access Memory and a Magnetoresistive Random Access Memory.

8. **(Currently Amended)** A semiconductor memory card according to Claim [[5]] 1,

wherein

the internal memory of the tamper resistant module includes a first memory module and a second memory module, and

a unit of writing in the second memory module is smaller than a unit of writing in the first memory module, and the second memory module stores file management data.

9. **(Original)** A semiconductor memory card according to Claim 8, wherein

the second memory module is one of a Ferroelectric Random Access Memory and a Magnetoresistive Random Access Memory.

10. **(Previously Presented)** A semiconductor memory card according to Claim 1 being a multi-application memory card, wherein

the program is one of a plurality of applications with which the memory card is compatible, and

the internal memory has a plurality of usage areas corresponding one to one to the applications.

11. **(Previously Presented)** A semiconductor memory card according to Claim 10, wherein

at a time of addition of one of the applications to the memory card, the processing unit assigns an area to be used by the added application.

12. **(Currently Amended)** A semiconductor memory card according to Claim 1, wherein the assigned area in the ~~nontamper resistant~~ nonvolatile memory that is not tamper resistant is a file system in which files are stored.

13. **(Original)** A semiconductor memory card according to Claim 1, wherein the tamper resistant module includes a CPU that executes the program.

14. **(Original)** A semiconductor memory card according to Claim 1 including a host interface which is an interface with a device connected to the memory card, wherein

the host interface judges whether a command from the device is an expansion command, and

the program starts, if the command is judged to be the expansion command.

15. **(Currently Amended)** A semiconductor memory card of Claim 1 including a plurality of file systems, a secure level of each of the file systems being one of high, medium, and low, wherein

a first file system whose secure level is high is stored in the tamper resistant module,

a second file system whose secure level is low is stored in the ~~nontamper resistant~~ nonvolatile memory that is not tamper resistant, and

the total area that is a combination of the usage area in the tamper resistant module ~~memory~~ and the assigned area in the ~~nontamper resistant~~ nonvolatile memory that is not tamper resistant composes a third file system whose secure level is medium.

16. **(Currently Amended)** A controlling program in a semiconductor memory card that comprises a tamper resistant module and a ~~nontamper resistant~~ nonvolatile memory that is not tamper resistant, and that is executed by a CPU in the tamper resistant module,

wherein the tamper resistant module includes: an internal memory having a usage area used by an application stored in the tamper resistant module; a virtual machine; and an operation system, the application being executable by the virtual machine,

wherein the controlling program is operable to (i) assign an area in the ~~nontamper resistant~~ nonvolatile memory that is not tamper resistant to the application, and (ii) generate, [[on]] in the internal memory of the tamper resistant module, access information for the assigned area in the ~~nontamper resistant~~ nonvolatile memory that is not tamper resistant, ~~and~~

wherein the assigned area in the ~~nontamper resistant~~ nonvolatile memory that is not tamper resistant is for a portion of confidential data to be written in, the portion of confidential data being used by the program and read by referring to the access information existing in the internal memory of the tamper resistant module,

wherein the internal memory stores a first area table indicating a location and a size of the usage area,

wherein the nonvolatile memory that is not tamper resistant stores a second area table indicating a location and a size of the assigned area in the nonvolatile memory that is not tamper resistant, the second area table being encrypted using a predetermined encryption key, and wherein the access information is a set of the predetermined encryption key and information indicating a location of the second area table.